

WE CLAIM:

1. A network bridge having a malware scanner.

5

2. A network bridge as claimed in claim 1, comprising a data packet analyser operable to identify data packets received by said network bridge at least a portion of which are to be passed to said malware scanner for scanning.

10 3. A network bridge as claimed in claim 2, wherein said data packet analyser identifies data packets having a predetermined network layer protocol as to be passed to said malware scanner for scanning.

15 4. A network bridge as claimed in claim 3, wherein said predetermined network layer protocol is one or more of:

TCP/IP;

IPX;

SNA; and

Appletalk.

20

5. A network bridge as claimed in claim 2, wherein said data packet analyser identifies data packets having a predetermined application layer protocol as to be passed to said malware scanner for scanning.

25

6. A network bridge as claimed in claim 5, wherein said predetermined application layer protocol is one or more of:

SMTP;

FTP;

HTTP;

30

SMB; and

NFS.

7. A network bridge as claimed in claim 1, wherein said malware scanner is operable to concatenate portions of a data file from a plurality of data packets to form a data file to be scanned.

5 8. A network bridge as claimed in claim 1, wherein said malware scanner is operable to scan for one or more of:

computer viruses;

Trojans;

worms;

10 banned computer programs; and

banned words within e-mail messages.

9. A network bridge as claimed in claim 1, wherein data that has been scanned by said malware scanner is forwarded to its intended recipient.

15 10. A network bridge as claimed in claim 1, wherein said malware scanner is formed of one or more of:

a software based malware scanner; and

a hardware based malware scanner.

20 11. A network bridge operable to intercept one or more data packets, to forward at least a portion of said data packets to a malware scanner for scanning, and to forward data from said data packets after scanning to its intended recipient.

25 12. A network bridge as claimed in claim 11, comprising a data packet analyser operable to identify data packets received by said network bridge at least a portion of which are to be passed to said malware scanner for scanning.

30 13. A network bridge as claimed in claim 12, wherein said data packet analyser identifies data packets having a predetermined network layer protocol as to be passed to said malware scanner for scanning.

14. A network bridge as claimed in claim 13, wherein said predetermined network layer protocol is one or more of:

TCP/IP;
IPX;
SNA; and
Appletalk.

5

15. A network bridge as claimed in claim 12, wherein said data packet analyser identifies data packets having a predetermined application layer protocol as to be passed to said malware scanner for scanning.

10 16. A network bridge as claimed in claim 15, wherein said predetermined application layer protocol is one or more of:

SMTP;
FTP;
HTTP;

15 17. A malware scanner operable to receive at least a portion of one or more data packets intercepted by a network bridge, to concatenate said data packets into a data file to be scanned and to forward said data file after scanning to its intended recipients via said network bridge.

20 18. A malware scanner as claimed in claim 17, wherein said malware scanner is operable to scan for one or more of:

25 computer viruses;
Trojans;
worms;
banned computer programs; and
banned words within e-mail messages.

30 19. A malware scanner as claimed in claim 17, wherein said malware scanner is formed of one or more of:
a software based malware scanner; and
a hardware based malware scanner.

10 20. A method of malware scanning comprising the steps of:
receiving data packets at a network bridge;
sending at least a portion of said data packets from said network bridge to a
malware scanner;
concatenating data received by said malware scanner to form a data file to be
scanned;
scanning said data file with said malware scanner; and
forwarding said data file after scanning via said network bridge to its intended
recipient.

15 21. A method as claimed in claim 20, comprising the step of identifying data
packets received by said network bridge that are to be passed to said malware scanner
for scanning.

20 22. A method as claimed in claim 21, wherein data packets having a
predetermined network layer protocol are identified as to be passed to said malware
scanner for scanning.

25 23. A method as claimed in claim 22, wherein said predetermined network layer
protocol is one or more of:
TCP/IP;
IPX;
SNA; and
Appletalk.

30 24. A method as claimed in claim 21, wherein data packets having a
predetermined application layer protocol are identified as to be passed to said
malware scanner for scanning.

25. A method as claimed in claim 24, wherein said predetermined application
layer protocol is one or more of:
SMTP;
FTP;

HTTP;
SMB; and
NFS.

5 26. A method as claimed in claim 20, wherein said scanning scans for one or more
of:

computer viruses;
Trojans;
worms;
10 banned computer programs; and
banned words within e-mail messages.

27. A method as claimed in claim 20, wherein said malware scanner is formed of
one or more of:

15 a software based malware scanner; and
a hardware based malware scanner.